Business Improvement Project:

How to Assist in Increasing Compliance

with the

Freedom of Information and Protection of Privacy Act

A Joint Project of the
Office of the Information and Privacy Commissioner/Ontario

and the

Ministry of Health and Long-Term Care
Freedom of Information and Protection of Privacy Office

Information and Privacy
Commissioner/Ontario

Ministry of Health
and Long-Term Care

April 2003

The Information and Privacy Commissioner/Ontario would like to acknowledge the work of Dr. Carolyn Lentz, Manager, Freedom of Information and Protection of Privacy Office, Corporate Management Branch, Corporate Services and Organizational Development Division, Ministry of Health and Long-Term Care.

This publication is also available on the IPC Web site.

Cette publication est également disponible en français.

Information and Privacy Commissioner/Ontario
80 Bloor Street West, Suite 1700
Toronto, Ontario M5S 2V1
416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: www.ipc.on.ca

Ontario

Ministry of Health and Long-Term Care
Corporate Services and Organizational Development Division
Corporate Management Branch
Freedom of Information and Protection of Privacy Office
5700 Yonge Street, 5th floor
Toronto, Ontario M2M 4K5
General Inquiry: 416-327-7040
Fax: 416-327-7044

Table of Contents

Introduction 1

Business Improvement Project Overview 2

Components of the FIPPO Business Improvement Project 3

- Placement 3
- Organizational Capacity 3
- Case Management System 4
- Accountability 4
- Processes 4
- Communications and Training 5

Moving Forward – Continuous Improvement 7

Appendix A – Freedom of Information and Protection of Privacy (FIPP) Fact Sheet 9

Appendix B – Handling and Security of Confidential Information – Self-Assessment for Managers 13

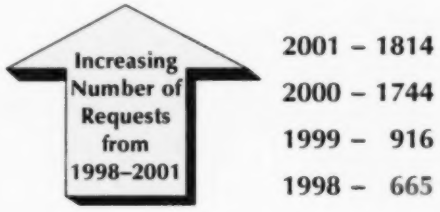
Introduction

In 2000–2001, the Freedom of Information and Protection of Privacy Office (FIPPO) in the Ministry of Health and Long-Term Care (MOHLTC) undertook a business improvement project that included a number of components. This paper provides a brief overview of the project and focuses in more detail on a key element: communications and training for the various client groups in the ministry to promote a shared understanding and accountability for compliance with the *Freedom of Information and Protection of Privacy Act*.

Business Improvement Project Overview

The Ministry of Health and Long-Term Care is a large, decentralized ministry. Health care is a high priority for the public, and the ministry has a heavy reform agenda with many high profile government commitments to deliver. There are a number of challenges managing a FIPP function in this environment.

The ministry holds large volumes of personal health information as a result of its service delivery. Security, confidentiality and privacy protection of the personal information holdings and databanks are critical issues for the ministry.



The ministry receives a significant volume of access requests that have been steadily increasing over the last few years. Many of these requests are complex and reflect the heightened public, stakeholder and media interest in health-related matters, as well as requests for personal information.

A few years ago, the ministry started experiencing some challenges in meeting its statutory 30-day compliance requirement for dealing with access requests as a result of dramatic increases in the volume of requests.

Following the IPC's annual report in 2000, which indicated a low compliance rate for the ministry, the IPC and the ministry undertook a joint initiative to explore ways to improve the rate of compliance.

The FIPPO embarked on an improvement project with the help of the ministry's Business Improvement Office and a small advisory group to ensure it had the right organizational structure and capacity, the right processes, tools and other supports for a high-performing FIPPO that could in turn support the ministry in meeting its obligations under the *Act*.

Components of the FIPPO Business Improvement Project

Placement

We looked at where would be the best place for the FIPPO to reside in the ministry to ensure appropriate functional alignment.

A decision was made to transfer the Office from the Legal Services Branch to the Corporate Management Branch in the Corporate Services and Organizational Development Division.

Organizational Capacity

Given the increasing workload, we also reviewed the organizational capacity and resources of the FIPPO. In determining the appropriate number of resources and the structure of the office, we built succession capacity into the organizational model. A team leader position was established to support the Manager, and a junior advisor position was set up as an entry level professional position to deal with the more routine requests and to free up more of the senior advisors time for the more complex files. Training was also provided for FIPP Office staff. This is ongoing as we continue to build a more comprehensive learning program with curriculum and modules based on a clear definition of core knowledge, skills and behaviours required for a high-performing advisor. Learning is focused on deepening knowledge of the *Act*, especially privacy, and enhancing interpretative skills; increasing knowledge of the ministry's organization, its diverse businesses and records; improving advisory, negotiation, and influencing skills for effective client service.

Case Management System

The high volume of requests warranted a more efficient method of tracking and monitoring. We investigated a few options for a new case management, tracking and reporting system, and went with the system used by the Ontario Ministry of Natural Resources as well as most federal departments for their FOI and privacy administration.

The system is called ATIP, a product of PRIVASOFT, which has been specifically developed for use in FOI and Privacy offices. The case management system, ATIP flow, captures real-time information on the status and workflow of the FOI processes, acknowledgements, searches for records, third-party notifications, decisions, and appeals.

The system also permits prompt assignment of requests and responsibilities, automated correspondence, and consolidates notes, response documents and actions taken for easier search and retrieval. The case management reports and information help to quickly identify problems and allow for more prompt resolution.

Another part of the system, ATIP image, also includes document imaging capabilities, which electronically severs text and builds an electronic index of the access decisions. This function cuts down on time-consuming photocopying, manual severing and paginating. Electronic search and checking features help to identify duplicate or similar documents to ensure that they are treated in the same manner.

This tool is helping staff shift their focus and time to their advisory role rather than manually processing paper. The system will also be able to easily provide regular reports to each division's senior management in the ministry to help them with their own monitoring and interventions.

Accountability

Accountabilities, roles and responsibilities were more clearly defined for the FIPPO; for the network of program area contacts who are responsible for searching records in each of the ministry divisions/ branches; for decision makers, and for legal and communications branches. The message was reinforced that achieving compliance is a ministry-wide responsibility, not just the responsibility of the FIPP Office.

Processes

We looked at opportunities to enhance ministry processes and support for FOI and privacy. For example, the FIPP Office attends the ministry Executive Assistants' committee meeting each week for file review and discussion on issues to be addressed.

We worked with the Legal Services Branch to streamline processes and working relationships, and with the Communications and Information Branch to streamline the management of access and privacy issues.

Communications and Training

We developed a number of products and undertook activities to improve awareness and understanding about FOI and privacy within the ministry.

Our communications and training objectives were to:

- provide a "FIPPA 101" refresher on the basic access and privacy provisions of the *Act*, and explain the processes and timelines to be followed within the ministry
- clearly articulate roles and responsibilities, and
- ensure people understood FIPP Office's services and support, and what we were trying to achieve through the business improvement project

Our key target audiences were Program Area Contacts (PACs - the network of contacts for the FIPP Office in each division and branch of the ministry); decision makers (Directors, Executive Directors and Assistant Deputy Ministers), managers and staff.

We reinforced the message that FIPPA is based on the fundamental principles of openness and accountability and plays a key role in strengthening our democratic form of government. We also emphasized that the business improvement project was part of our ongoing commitment to quality service, and to ensure that we are able to meet our obligations to comply with the letter and spirit of the *Act*.

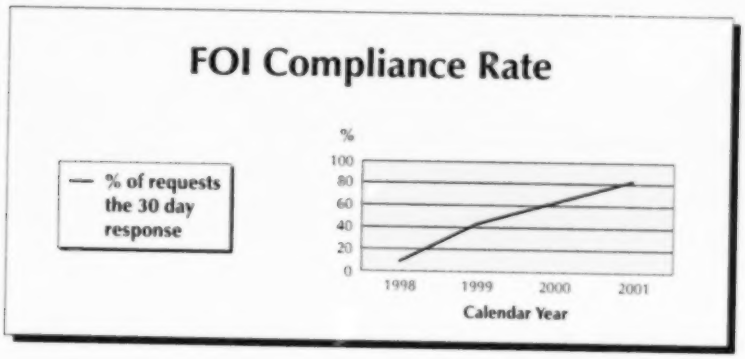
Communications activities and products included:

- Memos from the Deputy Minister to all staff, reinforcing the messages noted above
- Fact Sheets outlining the key elements and principles of the *Act*, the ministry's responsibilities, the role of the Office of the Information and Privacy Commissioner, the appeals process, and various facts and tips for staff (see MOHLTC sample, Appendix A, page 9)
- We made use of the ministry's employee newsletter "Inside Health" and published articles on FOI and highlighting the progress of the business improvement initiative.
- We developed an intranet web site that includes information sheets, toolkits and templates for the program area contacts and decision makers. There are also links to other web sites such as the IPCO and the corporate Ontario Management Board Secretariat site for information on appeal decisions and privacy protection resources.
- In partnership with other corporate areas in the ministry, we developed a self-assessment tool and best practices guide for managers on security, confidentiality and privacy of information (see MOHLTC sample, Appendix B, page 13).

Training activities and products included:

- Training modules for Program Area Contacts (PACs) that covered their roles and responsibilities, strategies for dealing with large and complex requests, and how to effectively communicate decisions on access. The FIPPO organized and delivered the PAC training sessions and continues these sessions for new PACs.
- A decision maker orientation module that focused on the roles and responsibilities of senior executives and directors as decision makers. The FIPP Office attended senior management committee meetings for each division of the ministry to roll this out.
- We offered, and responded to requests, to come to branch management and staff meetings as required to deliver presentations. We also provided orientation sessions for new political staff in the Minister's Office and Associate Minister's Office.

In 2001, despite continued high volume of FOI and other requests (approximately 2,000), the ministry increased it compliance another 20% over the previous year for a total of 83.3% – the highest compliance rate ever achieved in MOHLTC.



Moving Forward – Continuous Improvement

2002 has been a challenging year to sustain improvements and compliance rates given the Ontario Public Service labour disruption, however we will continue improvement efforts in the following areas:

- Ongoing communications and training for new PACs, decision makers, managers and staff
- Developing internal customer surveys to evaluate the quality of the ministry's FIPP Office services, processes, products and relationships to determine further areas for improvement
- Relationship building within the ministry and externally (e.g. networking, sharing of best practices and active participation in Ontario Public Service corporate FIPP initiatives)
- Process mapping and documentation in the FIPP Office to identify process improvements, for consistency, and to use for orientation of new staff
- Ongoing FIPP Office staff development to build expertise for strategic advice and effective service delivery

For further information, please contact:

Dr. Carolyn Lentz, Manager
Freedom of Information
and Protection of Privacy Office
Corporate Management Branch
(416) 327-2361

Angela Coke, Director
Corporate Management Branch
(416) 326-5725

Corporate Services and Organizational Development Division
Ontario Ministry of Health and Long-Term Care

Appendix A

Freedom of Information and Protection of Privacy (FIPP) Fact Sheet

Freedom of Information and Protection of Privacy (FIPP) Fact Sheet

What is Freedom of Information and Protection of Privacy (FIPP)?

The *Freedom of Information and Protection of Privacy Act* (the *Act*) gives individuals the right to request access to government information, including most general records and records pertaining to their own personal information. At the same time, the *Act* requires that the government protect the privacy of an individual's personal information existing in government records.

The FIPP *Act* is based on the following principles:

- Informed citizens are essential to the democratic process
- Openness in government is essential to accountability and the *Act* is an integral part of that process
- Everybody has the basic right of access to their personal information which is collected and used by government

The Ministry's Responsibilities

As a provincial ministry governed by the *Act*, we must:

- Design and implement record systems that adequately protect personal privacy and confidential records. The *Act* includes rules regarding the collection, retention, use, disclosure and disposal of personal information in its custody or control
- Protect records from inadvertent destruction or damage.
- Protect the confidentiality and security of personal information, Cabinet and Executive Council information, or third-party information.
- Respond to access requests within the legislated 30-day time frame and either make records available, deny access or cite extraordinary circumstances resulting in delay. (Program Areas have 20 calendar days to forward their response to the Ministry FIPP Office – 15 calendar days if it is a sensitive request). The response must include written reasons for any denial and inform requesters of their right to appeal the decision.
- Respond to requests for the correction of personal information.
- Where necessary, defend decisions made under the *Act* in appeals.

The Information and Privacy Commission and Appeals

- The *Act* gives people the right to appeal decisions to the Information and Privacy Commissioner/Ontario (IPCO).
- The IPCO is an independent adjudicative tribunal that conducts inquiries and inspects records; they may either uphold a ministry decision or issue a legally binding decision regarding disclosure.
- The FIPP Office coordinates the ministry response to IPCO appeals and represents the ministry in the mediation process.
- IPCO also investigates privacy complaints.

FOI Facts and Tips

The Ministry's volume of requests is increasing:

- 665 requests in 1998
- 916 requests in 1999
- 1,714 requests in 2000
- 1,814 requests in 2001

If an FOI request comes to your desk, ask yourself:

- Is there a clear sense of what the requester wants? If not, clarification of the request will save time and effort.

Keep the following in mind:

- Almost everything is a record and can be part of an FOI request.
- Your notes are not personal information and can be part of an FOI request – so take notes but use good judgement.
- E-mails are records and may be part of an FOI request.

Remember that assistance is available:

- If you have questions or concerns, contact your Program Area Contact or a Program Advisor in the FIPP Office immediately.

Who to Contact

If you have questions or concerns about the Ministry's Freedom of Information process please call the Freedom of Information and Protection of Privacy Office at:

(416) 327-7040

Appendix B

Handling and Security of Confidential Information

Self-Assessment for Managers

CMB

Corporate Management Branch

Handling and Security of Confidential Information

Self-Assessment for Managers

Ministry of Health and Long-Term Care

2001

Handling and Security of Confidential Information

Contents

Introduction 1

Roles and Responsibilities 2

Ministry Contacts 3

Management Controls/Accountabilities 4

Physical Security 5

Document Security 7

Cabinet Documents/Submissions 8

Electronic Data/E-Mail Security 9

Fax Machine Security 10

Voice Communication Security 11

Appendix A — Related Web Sites 12

Handling and Security of Confidential Information Self-Assessment for Managers

Introduction

Ministry of Health and Long Term Care (MOHLTC) employees are often required to prepare or handle sensitive information that is confidential. The risk of such information being accessed and inappropriately used by unauthorized individuals or organizations needs to be addressed and effectively managed.

This self-assessment document, the accompanying tip sheets and list of related web sites has been prepared to assist managers in ensuring that confidential information is not disclosed to any unauthorized person or organization and that effective procedures are in place for the secure handling and storage of these documents.

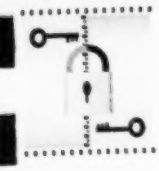
These tools and resources will:

- support the requirements of the OPS Oath of Office and Secrecy that all employees agree to abide by;
- support managers and employees by providing direction on how to ensure the integrity of confidential information and by outlining their responsibilities;
- ensure that access to confidential documents is limited to authorized staff and that such documents are not used for purposes other than what was originally intended; and
- provide assistance to program areas in the development of internal procedures related to the handling and security of confidential information.

Roles and Responsibilities

Program Managers are responsible for:

- meeting their obligations under the Conflict of Interest and Post-Service Directive for Public Servants and Public Officials, the *Freedom of Information and Protection of Privacy Act (FIPPA)*, and the Oath of Office and Secrecy, to protect any confidential information under their control or custody from unauthorized disclosure to any person or organization;
- reviewing applicable legislation and/or guidelines, processes and procedures, relating to the security of documents which applies to their program area;
- developing and maintaining internal procedures that support the requirements for the effective handling and security of confidential information;
- ensuring that all confidential information under their control is identified, handled and protected by reasonable security measures;
- ensuring that confidential information under their control or custody is protected from physical damage and from unauthorized access, alteration, removal or destruction;
- ensuring that all confidential information under their immediate control has defined appropriate retention periods and is scheduled in a manner consistent with government policies, legislation and guidelines on records retention;
- ensuring the timely transfer or secure disposal of the confidential information in their custody in accordance with records retention schedules and government-wide standards;
- regularly reviewing this information with staff and making them aware of their obligations under the Conflict of Interest and Post-Service Directive for Public Servants and Public Officials, FIPPA and the Oath of Office and Secrecy, to protect any confidential information from unauthorized disclosure to any person or organization; and
- ensuring that staff are aware of, trained and understand applicable legislation and/or guidelines, processes and procedures related to the security of confidential documents which applies to their program area.



Employees are responsible for:

- meeting their obligations under the Conflict of Interest and Post-Service Directive for Public Servants and Public Officials, the *Freedom of Information and Protection of Privacy Act (FIPPA)*, and the Oath of Office and Secrecy, to protect any confidential information under their control or custody from unauthorized disclosure to any person or organization;
- reviewing and understanding applicable legislation and/or guidelines and procedures related to the security of confidential documents which applies to their program area;
- ensuring that all confidential information under their control or custody is identified, handled and protected in accordance with internal procedures and processes;
- ensuring that confidential information under their control or custody is protected from physical damage and from unauthorized access, alteration, removal or destruction in accordance with internal procedures and processes; and
- advising their managers immediately if the security of confidential information has been breached and/or compromised.

Ministry Contacts

For information related to:

Cabinet Submissions, Corporate Coordination Office – general inquiry number (416) 327-8530

Freedom of Information and Protection of Privacy – general inquiry number (416) 327-7040

IT Security, IT Security Policy Specialist – (613) 548-6613

Physical Security, Facilities Management Services – general inquiry number (416) 327-7189

Management Controls/Accountabilities

		Yes	No
1.	Has a security awareness plan been developed and implemented for managers and staff?		
2.	Are security policies, procedures and standards communicated to staff?		
3.	Does management periodically remind staff and/or others using the information e.g. consultants, of their obligations with respect to securing confidential and sensitive information?		
4.	Does management periodically remind staff of their responsibilities with respect to the Oath of Office and Secrecy?		
5.	Have staff and/or others using the information been informed and/or trained in the access and privacy provisions of Freedom of Information and Protection of Privacy Act (FIPPA)?		
6.	Are exit interviews conducted with terminating employees to remind them of confidentiality obligations and to retrieve appropriate physical assets (e.g. keys, passcards, etc.)?		
7.	If third parties have access to confidential information, (e.g. mail, shredding, I & IT that has been outsourced) have roles, responsibilities, ownership, confidentiality, consequences for violations, and specific security obligations been outlined?		

Physical Security

		Yes	No
1.	Is there a process to control visitor access to areas where confidential documents are worked on or stored?		
2.	Are unknown persons seen in operational areas challenged/questioned by staff (e.g. Can I help you, Are you looking for someone, etc.)? Are staff aware that they should not allow people to follow them into their workplace unless that person is known to them and has permission to be there?		
3.	Is the entrance to your work location locked after normal business hours?		
4.	Do all staff have access to secure furniture/equipment to store paper/ electronic files and personal effects?		
5.	Is information protected during business and non-business hours from being physically accessed by non-authorized persons?		
6.	Are confidential papers secured/locked away by staff when not in use and at the end of the day?		
7.	Is there a "clean desk" policy when staff leave at the end of the day?		
8.	Are file rooms containing confidential and sensitive information kept locked when not being accessed?		
9.	Are keys to locked file cabinets and locked areas controlled and monitored?		
10.	Are staff aware that they are responsible for protecting their security access cards and that damage or theft to the card is to be immediately reported to their manager?		

Physical Security – continued

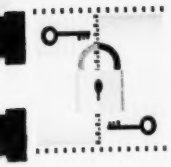
		Yes	No
11.	Are keys/access cards of exiting employees routinely collected?		
12.	When applicable, are combinations to locks changed on a regular basis? Are they changed when staff leave the branch/program/facility?		
13.	Are new combinations given to authorized users in a confidential way?		
14.	Are delivery staff (e.g. couriers, mail and other delivery staff) escorted at all times during their transactions?		
15.	Is there a mechanism/process in place to identify and notify management of security violations? Is this process timely?		
16.	Are users aware of the process required if they discover that information/ security has been compromised?		
17.	Does management take the necessary action to address information security violations and strengthen procedures as required?		

Document Security

		Yes	No
1.	Are confidential or sensitive documents identified and marked as such?		
2.	Is information accessible only to persons whom management of the program area has authorized?		
3.	Is control exercised over the number of copies of confidential materials produced? Are they distributed on a "need-to-know basis" only?		
4.	Are all extra copies of confidential/highly sensitive materials collected after meetings?		
5.	Are drafts or duplicates that are no longer required shredded/deleted as soon as possible?		
6.	Are documents intended for destruction secured until disposed of? (In addition to paper documents, this includes magnetic media, microfiche, etc.)		
7.	Are confidential or sensitive documents shredded before being placed in recycling bins?		
8.	Are mechanisms in place to monitor and control the removal of confidential documents either to other ministry offices or off site (for work related purposes)?		
9.	Are envelopes used to enclose and mail confidential documents properly marked/identified?		
10.	Is information that is no longer required for business archived appropriately?		

Cabinet Documents/Submissions

		Yes	No
1.	Are mechanisms in place to clearly determine the confidential status of documents (e.g. use of stamps, header or footer to indicate "Confidential Document" or "Confidential Advice to Cabinet")?		
2.	Are all early versions of Cabinet Submissions/MB-20s, etc. marked "Draft" and version # at the top of each page?		
3.	Is the required proforma format used (e.g. "Confidential Document" or "Confidential Advice to Cabinet") for final versions of Cabinet and Management Board of Cabinet (MBC) documents?		
4.	Are designated ministry staff used for the transport of Cabinet Submissions/MB-20s?		
5.	Are double envelope procedures used to send Cabinet Submissions or other highly sensitive information outside the ministry?		
6.	Are staff discouraged from taking Cabinet Submissions for work to be done off-site?		

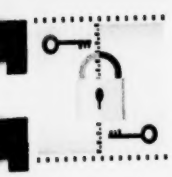


Electronic Data/E-Mail Security

		Yes	No
1.	Are computer screens situated on desks to avoid accidental screen viewing by passers by or visitors?		
2.	Are users instructed not to leave computers logged in and unattended?		
3.	Are staff informed that e-mail is not a secure network for sending confidential/sensitive information?		
4.	Is confidential or sensitive information being worked on in "draft mode" on a computer only printed when necessary?		
5.	Are isolated or dedicated printers used to print sensitive information to ensure confidentiality?		
6.	Are mechanisms in place to ensure that confidential information stored on networks is accessible only by those authorized to access the documents?		
7.	Are computers equipped with password protection to ensure unauthorized use is avoided?		
8.	Are passwords (including e-mail account passwords) changed regularly?		
9.	Are staff aware of, and do they follow, the policy of not allowing e-mail passwords to be shared?		
10.	Are computer passwords, e-mail accounts and access privileges of exiting employees' cancelled?		
11.	Are floppy discs/back-up tapes removed from computers and locked up when not in use or during off-hours?		
12.	Are hard drives overwritten – 10 times using specialized software – to ensure deletion when computer is returned to vendor or otherwise disposed of?		

Fax Machine Security

		Yes	No
1.	Are fax machines in an area not routinely accessible by visitors?		
2.	When using the fax machine to transmit confidential documents, are the documents clearly marked with either a watermark or stamp as "confidential"?		
3.	Are staff instructed to double-check numbers to avoid mis-dialing when sending confidential or sensitive information?		
4.	Is the receiving party notified ahead of time when confidential or sensitive information is being sent?		
5.	Is the receiving party called after the fax transmission to confirm the safe arrival of the fax?		
6.	Is there a copy of fax procedures (checking #s, calling before and after the transmission, etc.) posted beside the fax machine?		
7.	Do staff know how to use the security features (confidential mailbox) of the fax equipment to protect transmission and receipt of confidential information?		



Voice Communication Security

		Yes	No
1.	Are customers satisfactorily identified before discussing or releasing confidential information over the phone?		
2.	Are staff aware that they should not discuss confidential or sensitive information in voice mail messages?		
3.	Are staff aware that they should not use cellular or cordless phones to conduct any confidential or sensitive conversations?		
4.	Are staff aware that they should not allow someone calling from a cellular or cordless phone to discuss confidential information even if they are on a regular phone?		
5.	Are staff aware that they should not use a cellular or cordless phone to call in to their voice mail system to pick up messages?		
6.	Are staff aware that they should not use cellular or cordless phones to order anything by credit cards, specifically ministry credit cards?		

Appendix A — Related Web Sites

1. **Corporate Policy Branch** – http://intra.cpb.gov.on.ca

   This site contains corporate directives, operating policies and guidelines for administrative, financial and human resources functions. They are clustered into five key management areas: Accountability; Business Planning and Financial Management; Procurement; Information and IT Management; and, Human Resources Management.

   The Accountability Directive (found at the above site) lays the foundation for defining the standards for management practice in key areas such as financial management, human resources and administrative policies. It sets out an accountability framework (which includes definitions, key elements and principles) and the responsibilities of public servants.

2. **Recorded Information Management Directive** – http://intra.cpb.gov.on.ca/html/Mgmtrecd.html

   This is the complete directive on recorded information management. This site also links to the next two sites which contain fact sheets, bulletins, guidelines and best practices information.

   Fact Sheets – http://www.archives.gov.on.ca/english/rimdocs/index.html

   This location takes you to a series of fact sheets which refer to the Security and Integrity of Recorded Information.

   Information Bulletins – http://www.archives.gov.on.ca/english/rimdocs/infolist.htm

   These information bulletins explore special topics in recorded information management.

3. **Information and Information Technology Security Directive** http://intra.hsc.gov.on.ca/security

   This directive sets out the responsibilities and mandatory requirements for the implementation, management and control of information technology security within the ministry.

4. **Freedom of Information and Protection of Privacy Directive** (as it relates to *FIPPA*) – http://intra.cpb.gov.on.ca/html/Freinfpd.html

   FIPPA is a two part Act dealing with access to information and protection of personal privacy. The Act covers the Ontario government including ministries, agencies, Cabinet Office and the Premier's Office.

5. **Information and Privacy Office** – http://www.gov.on.ca/MBS/english/fip

   This site contains information on confidentiality rules including the FOI legislation, an on-line manual and summary of Information and Privacy Commissioner's Orders.

6. **Conflict of Interest and Post-Service Directive for Public Servants and Public Officials** – http://intra.cpb.gov.on.ca/pdf/Coi.pdf

   Part 2 of this directive deals with Mandatory Requirements of Conflict of Interest Provisions for all Public Servants.

7. **Injury, Illness and Employment Accommodation regarding the Health Information Program** – http://intra.hropenweb.gov.on.ca

   The Health Information Program component of the corporate Injury, Illness and Employment Accommodation Program (IIEA) outlines the process for obtaining employee health information and the subsequent handling and storage requirements. Section 4.2 of the Health Information Program entitled "Document Management" provides options for the storage and handling of confidential employee health records.

8. **Occupational Health & Safety Act** – http://www.gov.on.ca/LAB/ohs/ohse.htm

   The *Occupational Health & Safety Act (OHSA)* states that no employer shall seek to gain access to a worker's health record without the worker's written consent unless it is to comply with another statute or to comply with a court order. As a result, ministries need to ensure the confidentiality and security of worker health information.

   The *OHSA* also outlines basic responsibilities regarding the confidentiality of information as it applies to members of Joint Health and Safety Committees.

9. ***Workplace Safety and Insurance Act (1997)*** – http://www.gov.on.ca/MBS/english/publications/statregs/contents.html

   Documents pertaining to workplace injury or illness are collected under the authority of the Workplace Safety and Insurance Act (WSIA), 1997 s.22,and Regulation 101 under the WSIA. All documents and records are confidential and maintained by the employer.

10. ***The Young Offenders Act*** – http://canada.justice.gc.ca/en/laws/Y-1

    Privacy requirements related to the release of confidential information on young offenders are contained in section 38 – Protection of Privacy of Young Persons through to section 45 – Non-Disclosure and Destruction of Records.

Information and Privacy Commissioner/Ontario
80 Bloor Street West, Suite 1700
Toronto, Ontario M5S 2V1
416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: www.ipc.on.ca

Ontario

Ministry of Health and Long-Term Care
Corporate Services and Organizational Development Division
Corporate Management Branch
Freedom of Information and Protection of Privacy Office
5700 Yonge Street, 5th floor
Toronto, Ontario M2M 4K5
General Inquiry: 416-327-7040
Fax: 416-327-7044